

## **Tarrant County Special Terms and Conditions**

### **1. CRIMINAL BACKGROUND CHECK:**

- A. If this contract requires that Vendor personnel access Tarrant County Data (either on-site or remotely) or access secure areas of Tarrant County Facilities, then Vendor personnel may be required to undergo a fingerprint-based Criminal Justice Information Services (CJIS) Background Check, a Human Resources Criminal Background Check, or a Sheriff's Criminal Background Check. Criminal Background Checks will be paid for by Tarrant County.
1. The Vendor must provide information, including, but not limited to, employee name, date of birth, a clear copy of employee's driver's license, and a copy of employee's social security card for each individual required to pass a Criminal Background Check.
  2. Award of a contract could be affected by the Vendor's refusal to agree to these terms.
  3. Failure of the Vendor to supply personnel who pass a Criminal Background Check could affect the award of the contract or could result in the termination of the contract. If termination occurs, Tarrant County shall receive a pro-rated return of any fees paid for the remainder of the contract.
  4. The Criminal Background Check applies to the individual and not the Company.
  5. Passing status must be maintained by Vendor personnel for duration of the contract.

### **2. INFORMATION TECHNOLOGY HOSTED OR CLOUD SOLUTION:**

- A. The following is applicable when Vendor is providing Information Technology a hosted or cloud solution. Failure of the Vendor to conform to the requirements could result in the termination of the contract. If termination occurs, Tarrant County shall receive a pro-rated return of any fees paid for the remainder of the contract term.

#### **1. Information Security Points of Contact**

The Vendor shall designate and maintain a primary point of contact ("Security Contact") responsible for receiving, evaluating, and responding to all information security related inquiries, notifications, and coordination arising under this contract. The Vendor shall provide the name, title, email address, and telephone number of its Security Contact to Tarrant County prior to the commencement of services and shall promptly notify Tarrant County in writing of any changes to such contact information.

Tarrant County designates the following individual as its primary point of contact for information security matters:

Name: Russ Scott  
Title: Chief Information Security Officer  
Email: [RDScott2@tarrantcountytx.gov](mailto:RDScott2@tarrantcountytx.gov)  
Telephone: 817-212-7468

Either Party may update its designated Security Contact by providing written notice to the other Party. All security-related communications shall be directed at the then current designated contacts.

#### **2. Confidentiality, Integrity, Availability (CIA)**

Vendor shall protect the Confidentiality, Integrity, and Availability (CIA) of all Tarrant County Data. All Tarrant County information must remain private and

permit redaction of protected information before publication. Strong encryption must be used with data at rest and in transit. Audit logs must be periodically reviewed for anomalies and if one is found, follow Breach Notification procedures. Audit trails cannot be altered.

### **3. Breach Notification**

Vendor agrees that upon discovery of unauthorized access to Tarrant County Data, Vendor shall notify Tarrant County both orally and in writing. In no event shall the notification be made more than forty-eight (48) hours after Vendor knows or reasonably suspect unauthorized access has or may have occurred. Vendor shall notify Tarrant County of any breaches related to third party vendors they use within forty-eight (48) hours, whether or not they believe themselves affected.

For purposes of this contract, an "Information Security Incident" includes any event involving unauthorized access, use, disclosure, modification, destruction, loss, or compromise of data; any security breach; any material deviation from required security controls; or any other event reasonably believed to pose a security risk to Tarrant County information or systems.

The Vendor's notification shall, to the extent known at the time, include:

- A general description of the incident
- The date and time of detection
- The nature and scope of affected systems, data, or accounts
- The steps taken or planned to contain, investigate, and remediate the incident

The Vendor shall cooperate fully with Tarrant County in the investigation, containment, and remediation of any such incident, including providing timely updates and access to relevant records, personnel, and systems as reasonably required.

Notification shall be directed to Tarrant County's designated Information Security Contact identified in this contract.

### **4. Data**

All Tarrant County Data will remain in the 48 contiguous United States at all times, unless pre-approved in writing by Tarrant County ITD. This includes primary systems and all backups, snapshots, disaster recovery, analytical processing, archives, and any physical or virtual media at rest. Data must not be maintained or accessible from any location outside the 48-State U.S. Region. Any type of change occurring in the vendor environment that impacts Tarrant County's accessibility to application resources or data needs to be communicated by Vendor in advance.

### **5. Patches**

Vendor shall provide and install up-to-date software patches to maintain industry level security standards. Software provided by Vendor to Tarrant County must be current General Availability (GA) and under a current supportability/release package. Deprecated software cannot be installed or maintained within the Tarrant County Environment.

## **6. Right to Audit**

**6.1 Vendor :** Tarrant County reserves the right to audit, upon reasonable prior notice, the information technology security controls, systems, policies, and related documentation of the Vendor. Such audits may be performed by Tarrant County, its authorized representatives, or an independent third party engaged by Tarrant County.

**1. Audit Triggers:** Tarrant County may initiate an audit under any of the following circumstances:

- A material change in the scope, nature, or volume of services performed under this contract.
- A change in ownership, executive leadership, or key management personnel of the Vendor.
- Any request by the Vendor for additional access privileges, expanded system integrations, or increased data-handling responsibilities.
- A suspected or confirmed security incident, breach, or material vulnerability involving the Vendor or its subcontractors.
- Significant modifications to the Vendor's IT infrastructure, hosting environment, or security controls relevant to the contracted services.
- Regulatory, legal, or contractual requirements necessitating verification of compliance.
- Periodic risk-based assessments conducted at Tarrant County's discretion.

### **2. Cooperation Requirement**

Vendor shall provide timely and full cooperation, including access to personnel, facilities, systems, data, and records reasonably required to complete the audit. Vendor shall promptly remediate any deficiencies identified.

**6.2 Vendor Data Centers:** Tarrant County reserves the right to audit vendor data centers which house Tarrant County Data or receive SSAE 16 SOC Type II audits from a reputable security advisory service firm (e.g. EY, Deloitte, KPMG, PWC, Coalfire, etc.). Vendor shall, at a minimum, provide Tarrant County, with a yearly Compliance Report attesting to the fact that they have conducted periodic reviews of their Audit Logs to include the Date & Time of review(s), any anomalies found with a brief description, and the disposition after investigation of the anomaly.